

~~SECRET~~ SECURITY INFORMATION
CLASSIFICATION
DRAFT FORM FOR CROSS-INDEX CARDS

Accession Number for file S- Location TL

Authority OC Sig O, European Theater of Operations

Title of Document (in caps) INTERROGATION REPORT COVERING PRISONER OF WAR, WERNER K.H. GRAUPE

Author Walter G. Fried, CAPT, SigC

Document Number TICOM/IR-47478, Part 2

Report Number IF 107

Date of Document 15 Nov '44

No. of Pages 10 p(p) or No. of items _____

incl. (check items included)

app. _____	disgr(s). _____	tb(s). _____	graph(s) _____
map(s) _____	photo(s). _____	port(s) _____	dup(s). _____
other _____			

bibl p(p). _____
(give pages inclusive as: bibl. p. 9; bibl. pp. 15-17)

cy 1 & cy(s) _____ or _____ (No. of) _____ cy(s) _____

CLASSIFICATION SECRET

ABSTRACT _____

I-FOLDER
107

SECRET

OFFICE OF THE CHIEF SIGNAL OFFICER
HEADQUARTERS
EUROPEAN THEATER OF OPERATIONS
APO 897 U.S. ARMY

Spillman
WJE
(F)

17/107

ETSIG-I/wjf/bg

15 November 1944.

SUBJECT: Interrogation Report covering Prisoner of War,
Werner K.H. Graupe.

TO : Colonel G.A. Bicher, Director, S.I.U.

1. Pursuant to your instructions, Major Neff, Captain Maass, ^{*Herbert H*} and the undersigned, interviewed the above named Prisoner of War at Seine Base Guard House, on 13 November, 1944.

2. The substance of our discussions and conclusions is set forth in the attached report.

3. Prisoner Herbert H.B. Schwartze, who deserted with Graupe, was not questioned because we learned from Graupe that he knew nothing about cryptography or cryptanalysis but acted merely as a translator.

4. I make the following recommendations -

a. That Graupe be held here for further questioning with respect to U.S. security violations.

b. That a copy of this report be forwarded to GC & CS, with the suggestion that the proper persons there pursue the interrogation of Graupe with respect to German cryptographic organization and personnel.

Walter J. Fried
WALTER J. FRIED
Captain, Signal Corps.

5-5106
DO NOT DESTROY
Return to the
Signal Corps
Headquarters
APO 897
U.S. Army

SECRET

SECRET

REPORT OF INTERROGATION ON WERNER K.H. GRAUPE

HISTORY

In 1935 Werner K.H. Graupe (hereinafter referred to as "G") attempted to emigrate to the United States but was unable to do so because he had not performed the requisite German Military Service. He entered the German Army in May 1935 for one year but thereafter his father died and he was released in November 1935. Subsequently he applied for a student visa to permit him to emigrate to U.S. and did emigrate in October 1936.

He attended the Acadia Academy, Church Point, Louisiana, from which he graduated in May 1937. "G" states that he had been under the impression that this was a college and found the high school curriculum very easy. Most of his time was spent in learning English.

He commenced working in May 1937 and held various jobs for short periods. He was injured and while in the hospital was visited by U.S. immigration officials who informed him that although his visa was good for two years he had no right to work since it was purely a student visa. He agreed to return to Germany and left the United States in June 1938.

After he returned to Germany "G" worked for the Ford Motor Company, Berlin. This was apparently deemed an essential occupation because he obtained exemption from military service until 1942. He was then called up for the Army and sent to the Russian front.

He endeavored to obtain an assignment to an interpreters' unit in May 1942 basing his request upon his knowledge of English. His request was granted and he was sent to an interpreters' reserve in Meissen. Shortly thereafter he was transferred to Berlin to a cryptographic school of the OKH at Mattai Kirchplatz 4. "G" remained at this Headquarters until April 1943. The balance of the year 1943 "G" worked on cryptanalysis of Spanish, Portuguese and Brazilian military traffic at Nach Fern Aufkl Komp 624. In August he attended a 14-day course in Berlin and then returned to his unit. This work was then taken over by No. 12 unit in Lucien to which he was transferred in January 1944. Some work was done on M-209 traffic but his unit continued to work on Spanish, Portuguese and Brazilian until June 6. After D-Day interception of this traffic ceased and cryptanalytic attention was devoted solely to American and English traffic. After D-Day, Hq K5 moved from St. Germain to Lucien at which time he became part of NAAST 5. In July he was transferred to the newly created Nach Nah Aufkl Komp 965 commanded by Oblt. Ernst Schmitz, which was detached from K5 to service Pz Gruppe 5.

After July he acted as purchasing agent rather than as a cryptanalyst for the Company and was apparently devoting most of his thoughts to ways and means of deserting. He actually did desert late in August, but lived in Paris as a civilian and did not give himself up to the U.S. military authorities until 18 October.

SECRET

SECRET

FACTS ABOUT GERMAN CRYPTOGRAPHIC ORGANIZATION
AND PERSONNEL

"G's" knowledge of the Headquarters cryptographic organizations in Berlin seems to be very scant. It is apparent that a high degree of internal security is maintained and that he was told no more than was necessary for the performance of his duties.

He advises that when he first went to the cryptographic school in Berlin in 1942 the total personnel of the outfit consisted of 20 officers and about 120-130 men. In addition there were 10-12 women, who acted in stenographic capacities. He advises that this was the total Army organization at that time, but that the Navy and the Air Force had similar organizations.

The cryptographic school was at Mattäi Kirchplatz 4. The Head of the Bureau was Major Mettig. A Major Harrens was in charge of security. The Cryptanalytic Branch was under Captain Herbrüggen. There were at that time about five cryptanalytic sub-divisions. Department No. 1 worked on U.S. traffic, department No. 2 on English, department No. 3 on French, Portuguese, Spanish and Brazilian, and department No. 4 on Italian. There was another department which worked on Arabic, etc. "G" believes that Russian cryptanalysis was handled in a separate building. The Head of Department No. 1 was Sonderführer z. Steinberg. His Assistant (whom "G" describes as more able) was Unteroffizier Luzius. Pfc. Gruber was "G's" instructor in cryptography and cryptanalysis. Sonderführer z. Kühne was the Head of Department No. 3. In connection with Department No. 4 "G" stated that work of a security nature was done on Italian traffic. As a result of the success of this work representations were made to the Italians and they were shown that their systems were not secure. "G" mentions that this work was later discontinued. In connection with this branch of the organization "G" mentioned a Captain Fiala, who was probably a German Liaison Officer to the Italians.

"G" pointed out that a great deal of German cryptanalytic work was later decentralized. The usual intercept company had a complement of 15 cryptanalysts.

The cryptanalytic unit in Paris was known as Headquarters No. 5 Unit.

"G" also mentioned a Department F, which was created in 1943. This was a Research Department and the personnel consisted primarily of mathematicians.

The Head of the cryptanalytic section at the Lucien Headquarters was Major Hentze, who was a mathematician. Sgt. Engelhardt was in charge of the work on the M-209.

"G" knows that there was an IBM Department at Berlin Headquarters, but he has no idea of the number or type of machines located there. He advises that the Hollerith Factory in Germany was destroyed in 1942 and thereafter no replacements of machinery could be obtained. He knows of no other type of machinery used for cryptanalytic work.

"G" also mentioned a Department No. 10, which was the German Security Department. He also mentioned Department 11 which worked on systems used by agents of Germany's enemies. He stated, however, that most of the knowledge

SECRET

about agents' cryptographic systems was derived from the Gestapo work rather than from cryptanalytic work.

CRYPTANALYTIC ACTIVITIES OF "G" AND HIS ASSOCIATES

At this point it should perhaps be stated that "G" seems to be highly intelligent, that the work he was doing was definitely above the "stooge" level, but that he was apparently not capable of what might be termed original high grade cryptanalysis. His position in the organization, however, furnished him with information about a great many activities in which he did not personally participate.

At cryptographic school in Berlin "G" studied simple cryptographic systems and methods of solution. One of Fletcher Pratt's books on cryptanalysis was used to some extent as a text book and apparently furnished a basis for the curriculum.

His class first studied monoalphabetic substitution, which he calls "single Caesar" and polyalphabetic substitution which he calls "spalten Caesar". They studied various types of transposition systems. He mentioned specifically systems in which various diagonal methods of inscription and transcription are used, and systems in which columns are transcribed alternately from top to bottom and from bottom to top. These he designated "snaking". Of course, he called substitution "Ersatz" and transposition "Versatz". They also studied substitution systems using two digits for each letter with the number of possible variants depending on the frequencies of the letters involved. Problems presented were typewritten and based on English military vocabulary.

They also studied a system which they call "EC5" (English Code No. 5) in which code values were written on a 25 x 25 rectangle and were represented by a diagraph consisting of the coordinates of the cell in which the value appeared. He mentioned that this type of system was later called SLIDEX and stated that at a later date he thought (but was not sure) that the size of the rectangle was only 9 x 12. He mentioned that the top coordinate was taken first and then the side coordinate.

As previously mentioned "G's" first work was on Spanish, Portuguese and Brazilian systems. He worked on Spanish military transposition and also on a Spanish digit cipher with variants.

When "G" returned to Berlin in August 1943 for a further course of training he studied the operation of the Hagelin machine. At this time Major Mattig was no longer in the OKH cryptographic unit. He had been transferred to the OKW unit which "G" believes had been newly created.

Despite the completion of this additional course "G" continued to work principally on transposition systems. Most of his work was apparently done on messages sent from Brazil to the U.S. by General Ciudad. He advises that five out of seven Brazilian systems were readable. He continued this work through the end of 1943.

During a period, which he did not specify (it may have been in Berlin, late in 1942), "G" worked on a U.S. strip system. He called this "Streifen verfahren". He advises that the traffic on which he worked emanated from Iceland and from the Caribbean area. In this system strips were never changed but the order of the strips was changed daily or every other day. Strips were not captured but the alphabets were reconstructed cryptanalytically. He does not know how this was accomplished but advises that a 25-page report on the solution was written by Steinberg and Luzius, who did the work. Later "G" conjectured that possibly the strips had been solved from circular messages. He realized that a pair of circular messages could be used for determining the daily key in exactly the same way as a crib could be used and his unit was on the lookout for circulars.

This is the M-94

"G's" work consisted simply of finding the daily key. Apparently a series of 25 charts was constructed. These may have been synoptic tables or something similar. Across the top of each chart was the plain alphabet, Down the left-hand margin of each chart were numbers from 1-25, corresponding to the 25 strips. The body of the chart contained for each clear letter the letters appearing on the 25 strips at the interval for which the particular chart was constructed. When the work was first started the daily key was found by assuming a beginning and trying in turn each one of the charts. Certain intervals were eliminated as impossible, and the further work consisted of trying all the remaining possibilities on other messages or other cycles of the same message. The beginning most usually assumed was "Request".

At a later date IBM cards were used for the purpose of eliminating impossible charts. There was a card for each plain-cipher diagraph. "G" stated that there were 625 cards, but it would seem that there must have been 650. For each card there were 25 positions which could be punched, corresponding to the 25 possible intervals. The card was punched for each interval that was possible, so that the average card probably contained approximately 20 punches. These cards were, in fact, nothing more than an index of the charts. If, for example, the letter "R" appeared under plain A on Chart 1, position 1 was punched on card AR. If there was no "R" under plain A on Chart No. 2, position No. 2 was not punched on the AR card. In order to utilize these cards a selection was made corresponding to the plain cipher pairs resulting from the crib assumption. These were then held up to the light and the only possible charts were those corresponding to the holes through which light showed. When "G" first discussed this matter he stated that there were only six holes per card but later, on reconsidering the matter, he thought that he was probably wrong and there must have been a great many more. He states that usually the card method eliminated all but two or three of the charts as possibilities. "G" advises that it usually took about two days to recover the order of the strips. He is quite positive that the same 25 strips were always used and that they were not drawn from a larger pool. He states that the traffic bore a five letter discriminant and they had up to 50 messages per day to work on. He advises that Steinberg and Luzius reconstructed strips only once and that no strips were ever captured. He advises also that most of the traffic read was practice traffic. Moreover, the traffic was often read by reason of the fact that the word "practice" appeared in the messages. "G" was under the impression that the strips were lettered and that the order of strips was determined by a key phrase. He did not describe precisely how this was accomplished. He stated that his unit frequently solved the literal

key after having reconstructed the order of the strips. He realized that this was unimportant from a cryptanalytic viewpoint but stated that they used to do it for fun. He remembers that one literal key read "Join the Navy and see the World". It seems that "G" must have been mistaken when he said that the strips were lettered because presumably they were numbered. Also it would seem that there must have been some compromise otherwise the numbers could not have been ascertained and it would have been impossible to recover literal keys.

"G" knew of what he called a 30-strip system but stated very definitely that it had never been solved.

Later "G" worked on the Division Field Code. One version of the D.F.C. was captured - he believes 19 or 21. This capture helped in the reconstruction of subsequent D.F.C.'s. He worked on North African D.F.C. traffic from Sicilian intercepts. The intercept station was at Taormina. He advises that they were never able to read the figure D.F.C. traffic, but the limitation of the literal version of the code enabled them to read it. One break was accomplished through a message reading "Draw supplies at _____". The first part of the message was in clear and the place name was spelled out in enciphered D.F.C. The word length enabled the place name to be identified and furnished them with a start in reconstructing the speller values of the code. He advises that when the D.F.C. was enciphered it was done by poly-alphabet substitution, using a reciprocal alphabet, with a period that was always a multiple of 4. He and his confreres felt that it was a grave mistake to have these period lengths and that the work would have been a great deal more difficult if some other periods had been employed.

Before describing his work on the Converter M-209 "G" advised us that a French Hagelin machine had been originally broken in 1940. He called this machine the C-36, and advises that it had fixed lugs (which he called cams) and that the kicks were always 1, 2, 4, 8 and 10. He stated, however, that the internal settings (which he called constellations) were changed only every few months. Solution was effected through the fact that nearly all messages started with "Refer". The original solution was accomplished from the beginnings of about 50 messages. He also advises that when the internal settings were changed the new traffic was sent to Berlin by courier and that Berlin was usually able to effect the solution within 48 hours.

"G" advises that the M-209 was not broken while he was in Berlin. The first break occurred in the Autumn of 1943. However, in June 1943 an M-209 key list for the month of June was captured in Sicily. The capture was not apparently reported because traffic was sent and read on the captured keys during the entire month of June.

The work of "G's" unit on M-209 traffic consisted entirely of breaking through depths. "G" knew that the M-209 internal settings were changed daily and that a number of keys were in use at the same time. His unit received 200-250 messages per day. "G" believes that the M-209 traffic is unbreakable except from depths. As far as "G" knows no solution was ever accomplished by the Germans from near depths, from stereotyped beginnings, or in any other way. He advises that in May 1944 they found depths on nine different days and were able to break eight of these days. He remembers specifically that discriminants PY and NC were broken. He was asked as to

whether any work was done on messages whose indicators agreed except for the index letter or except for one of the other six indicator letters, and replied that these messages were attacked on the theory that they were in truth depth and an error had been made in transmitting the indicator of one of them. He stated that the checking indicator at the end was not really a check because their intercept operators knew that there must be a check and consequently always forced an agreement in their intercepts. He was under the impression that the indicators were taken from lists and that there was a check off system and this accounted for their theory that approximately identical indicators did represent a true depth. The belief in a check-off system arose from the number of depths observed. It was thought, of course, that a depth resulted from a careless failure to check off.

"G" knew of the capture of some M-209 machines and some instruction booklets. He states that he recalled that the instructions provided that one wheel must have a kick of one, one wheel a kick of two and one wheel a kick of three or four and that all kicks must be possible. However, he states that he was not in Berlin at the time of arrival of the captured instruction book and consequently was a little vague as to the details of the instructions.

"G's" work consisted of reading the depth and reconstructing the pin and lug settings from the key derived. He realized that this obtained only relative pin settings; apparently others worked on trying to obtain the absolute values of the pin settings. He did not know how this was done except that he knew that "ZPAIENZ" was used in some manner in other messages after relative settings had been recovered to try to get the absolute settings. He advises that they always watched for a retransmission following a report of a message being indecipherable. Traffic analysis personnel was helpful in this regard. He knows of two cases in which a message was repeated with one wheel different and states that this helped in recovering the absolute settings.

Copies of all intercepts were sent to Berlin and apparently the cryptanalysts at Berlin Headquarters competed with those in the field in an effort to obtain solutions as rapidly as possible.

"G" advises that 60 elements of key were about the minimum necessary for reconstruction of pin and lug settings. He stated that it was possible with about 40 elements but very difficult. The technique of resolving key was the obvious one of writing out the key on all wheel periods and looking for the high kick wheels first. "G" called these "the big wheels". He advises that reconstruction of internal settings was much more difficult when the number of overlaps was heavy. He remembered two cases where key was derived from staggers rather than from ordinary depths. He states that he and his associates often wondered why the slide (which he described but did not designate by that name) had been eliminated from the original machine.

"G" advises that usually it took about two days to solve a depth and reconstruct the internal settings. Then it usually took two more days to derive the absolute settings. As a result of this and delays in obtaining intercepts it was usually at least a week before a day's traffic was fully out.

"G" apparently did some pure decoding after a day had been completely broken. He advises he was able, in decoding, to read a message even though two wheels were off.

"G" advises that a Doctor Linow, who was a Sergeant and a Mathematician, worked on the reconstruction of the M-209. Apparently he and Luzius and Steinberg determined the nature of the machine prior to its capture. "G" advises that the M-209 keys for the 82nd and 101st Airborne Divisions were captured in Normandy. These covered June 6, 7, 8, 9, 10 and 11. They were received by "G's" unit on June 9 from General Rundstedt's Headquarters at St. Germain. The capture was evidently not reported because the keys continued to be used and all traffic was read. "G" remembers one message in which General Taylor asked someone in London to send word to the U.S. advising that certain persons, whose names were listed, were safe.

MISCELLANEOUS INFORMATION
DERIVED FROM "G"

"G" advises that a code used by the U.S. Air Transport in Africa was solved. However, he worked on this very little, if at all. The code was two digit and was not mixed with plain language. He remembered that the value 12 introduced figures and that the value 55 introduced speller groups. The code was enciphered with a 10 digit additive. Here again he commented on the fact that if some other length of additive had been used the work would have been more difficult. The code was fully reconstructed and the additive regularly solved. He advises that the word "Accra" frequently appeared in the message. He also advises that this traffic, which passed in early 1943, discussed primarily the transportation of personnel. He remembers specifically one message which said something about the arrival of Mrs. McArthur and read in part "Extend all courtesy to Mrs. McArthur".

"G" advises that the British War Office code (which he called WOC) was reconstructed cryptanalytically and read until the code was captured in Africa. Afterwards a Doctor Liedtke worked for over a year to try to break the superseding system but was unsuccessful.

"G" advises that as far as he knows no American transposition traffic was ever solved. He knows that they were engaged in trying to find three messages of identical length in the same key, but were not successful in this search. This had been one of the methods used in solving Brazilian transposition.

"G" knows that there was a cryptographic section in the Foreign Office in Berlin but he does not know what sort of work was done by this organization.

"G" advises that Department "F", the Research Department, in Berlin, worked mostly on machines. He was informed that they had no success in working on the U.S. "big machine". He believes this machine was called the 211. He knows of no work that was done on any British machine systems.

"G" advises that traffic was being read on a compromised U.S. five-letter code which was called ACL. This was a two part code and messages were sent unenciphered. He did not know the nature of the traffic or who were the users. He stated that the code was still being used when he left Berlin.

"G" knew something about the replacement of Double Playfair by Raster.

SECRET

He stated that Oberinspector Kuhn (head of the teaching department in Berlin) had bet that he could break Double Playfair within six hours and had won his bet. "G" felt that Raster was a much improved system but rather too involved for the operators.

With respect to Russian military traffic "G" advises that in 1941 the Germans read practically everything but that by 1943 they were reading practically nothing.

"G" advises that as far as he knows the Germans do no security work on any Japanese traffic.

"G" did not know that the Hagelin machine was ever used by the Italians.

"G" once saw a printing type E machine. He never saw the type operated with lights and apparently knows nothing about the machine.

"G" had heard of the Fernschreiber but knew nothing about it and stated that it was used on landlines only.

"G" thought that there had been a big expansion of the German cryptanalytic organization in 1942. He advised that most of the men he knew had started work in 1942 or thereafter.

"G" advises that the British Slidex system was easily and regularly solved. He felt that it yielded quite valuable intelligence particularly as to bombing and artillery objectives. He also worked on a system called Codex which he thought was a U.S. system. This also was solved.

"G" suggested that the U.S. procedure for reporting captures of keys be tightened up. He seemed to feel that we were more lax in this regard than the Germans, and that this was a very grave menace to our cryptographic security.

"G" was under the impression that more M-209 traffic was being read than we imagined, this being due mainly to errors and breaches of security rather than the system itself. He felt, however, considering American traffic as a whole, that they were probably less successful than we anticipated.

CONCLUSIONS

"G" speaks excellent English and most of his information was very precise and clear. He had difficulty in finding words for some of the technical German cryptographic terms. There were, of course, a number of inaccuracies in his story. For example, he always called the M-209, the M-305. He was asked where he got that number from and said that he thought he had read it in a decode but that it might have been some other number.

He was fully cooperative and answered all questions freely and with apparent honesty. He explained that his cooperation was motivated by his belief that Germany had no chance of winning the war and that the sooner it was over the better.

In the course of the interrogation he constantly kept remembering new things. It was obvious that a great many of the things discussed had been out

SECRET

Authority EO 13526

SECRET

of his thoughts for a long period and that his recollection was being revived. It is highly probable that further interrogation will elicit a great many more facts. This report may point the way to gaps in his story, and to further questions that can be asked. It is suggested, therefore, that "G" be interrogated further in this Theater, particularly from the point of view of shedding further light on U.S. security violations.

There are people at GC & CS who have specialized in studying the German cryptographic organization. A great many of the statements made by "G" and the names mentioned by him will undoubtedly tie in with information they already possess. It will probably be useful to send a copy of this report to GC & CS and to provide an opportunity for further interrogation of "G" by the people who are expert in this field.

SECRET

Authority

EO. 13526